NOME E COGNOME:

MATRICOLA:

PROVA SCRITTA DI ALGEBRA 2, 23/01/2017

Esercizio 1 (10 punti) Sia $f = X^4 - 8X^2 + 1$, K il campo di spezzamento di f su $\mathbb{Q}$ e $L \subset \mathbb{C}$ il campo di spezzamento di f su $\mathbb{Q}[\sqrt{-2}]$.

a. Verificare che se α è una radice di f anche α^{-1} lo è.
b. Determinare $[K : \mathbb{Q}]$.
c. Determinare $[L : \mathbb{Q}[\sqrt{-2}]]$.
d. Determinare il campo di spezzamento di f su $\mathbb{Z}_{11}$.

Soluzione.

a. Basta osservare che $\alpha^4 f(\alpha^{-1}) = f(\alpha)$ e quindi se α è radice anche α^{-1} lo è.

b. Verifichiamo che f è irriducibile su $\mathbb{Q}$. Senz'altro non ha radici (le uniche possibili sono ± 1) e se proviamo a fattorizzarlo in $\mathbb{Z}[X]$ otteniamo

$$X^4 - 8X^2 + 1 = (X^2 + aX \pm 1)(X^2 - aX \pm 1)$$

da cui $\pm 2 - a^2 = -8$ che non ammette soluzione in $\mathbb{Q}$.

c. Osserviamo che $K \subset \mathbb{R}$. Cercando infatti le radici di f (sfruttando il fatto che è biquadratico) otteniamo $\pm\sqrt{4 \pm \sqrt{15}}$ che sono tutte reali. Osserviamo ora che

$$L = K[\sqrt{-2}]$$

e quindi che $[L : K] = 2$ visto che K, essendo reale, non può contenere $\sqrt{-2}$. Concludiamo che $[L : \mathbb{Q}] = 8$ e quindi $[L : \mathbb{Q}[\sqrt{-2}]]$ sfruttando la moltiplicatività del grado delle estensioni (lemma della torre).

d. Su $\mathbb{Z}_{11}$ il polinomio f si fattorizza nel seguente modo:

$$f = (X^2 - 2)(X^2 - 6)$$

e osserviamo che 2 e 6 non sono quadrati in $\mathbb{Z}_{11}$. Ricordando che $\mathbb{F}_{11^2}$ contiene le radici quadrate di tutti gli elementi di $\mathbb{Z}_{11}$ abbiamo che il campo di spezzamento è proprio $\mathbb{F}_{121}$.

Esercizio 2 (12 punti) Sia $A = \mathbb{Z}[\sqrt{-2}]$ e $\alpha = 20 - 5\varepsilon$.

a. Determinare una scomposizione in fattori irriducibili di α.
b. Mostrare che $A/(\alpha)$ ha un numero finito di ideali.
c. Descrivere gli ideali massimali di $A/(\alpha)$.
d. Quali campi possono essere ottenuti come quoziente di $A/(\alpha)$?

Soluzione.

a. Abbiamo $\alpha = 5(4-\varepsilon)$ e osserviamo che 5 è irriducibile perchè non esistono elementi di norma 5. Abbiamo inoltre $N(4-\varepsilon) = 18$ e quindi i possibili divisori di $4-\varepsilon$ devono avere norma che divide 18. Di norma 2 abbiamo solo ε (e associati) e proviamo a vedere se ε è un divisore di $4-\varepsilon$. Abbiamo

$$(4-\varepsilon)\frac{\varepsilon}{2} = 1 + 2\varepsilon$$

e quindi $(4-\varepsilon) = \varepsilon(1+2\varepsilon)$. Proviamo quindi a fattorizzare $(1+2\varepsilon)$ che ha norma 9. Gli elementi di norma 3 sono $1-\varepsilon$ e $1+\varepsilon$) (e associati). Proviamo a vedere se $1-\varepsilon$ divide $(1+2\varepsilon)$: otteniamo $1+2\varepsilon = (1-\varepsilon)^2$ e quindi la fattorizzazione in irriducibili di α è

$$\alpha = 5\varepsilon(1-\varepsilon)^2.$$

b. $A/(\alpha)$ è un anello finito (ogni classe è ha un rappresentante di norma minore di $N(\alpha)$ e chiaramente esistono un numero finito di elementi che hanno norma minore di $N(\alpha)$. In alternativa possiamo anche descrivere questi ideali esplicitamente: sappiamo che gli ideali di un quoziente $A/(\alpha)$ sono dati da $J/(\alpha)$ dove J è un ideale di A che contiene (α). Ne segue che J é generato da un divisore di α e questi sono in numero finito (e sono 1, 5, ε, $1-\varepsilon$, $(1-\varepsilon)^2$, 5ε, $5(1-\varepsilon)$, $\varepsilon(1-\varepsilon)$, e α).

c. Gli ideali massimali sono dati dagli ideali massimali che contengono α: sono quindi quelli generati dai fattori irriducibili di α e sono quindi

$$\frac{(5)}{(\alpha)},\ \frac{(\varepsilon)}{(\alpha)},\ \frac{(1-\varepsilon)}{(\alpha)}.$$

d. Un quoziente A/I di un anello è un campo se e solo se I è massimale. Nel nostro esempio abbiamo che i possibili campi sono

$$\frac{A/(\alpha)}{(5)/(\alpha)} \cong \frac{A}{5} \cong \mathbb{F}_{25}$$

dove abbiamo usato il terzo teorema di omomorfismo e il fatto che questo campo ha caratteristica 5 (infatti $5 = 0$). Similmente si ottengono gli altri due possibili quozienti

$$\frac{A/(\alpha)}{(\varepsilon)/(\alpha)} \cong \frac{A}{\varepsilon} \cong \mathbb{Z}_2$$

e

$$\frac{A/(\alpha)}{(1-\varepsilon)/(\alpha)} \cong \frac{A}{1-\varepsilon} \cong \mathbb{Z}_3.$$

Esercizio 3 (10 punti) Sia A un dominio e Q il suo campo dei quozienti. Un sottoinsieme $S \subset A$ si dice moltiplicativo se $1 \in S$, $0 \notin S$ e S è chiuso rispetto al prodotto di A. Siano S, S' sottoinsiemi di A moltiplicativi.

a. Mostrare che
$$A_S = \left\{ \frac{a}{s} \in Q : a \in A,\, s \in S \right\}$$
è un sottoanello di Q.

b. Mostrare che se $S \subset S'$ e ogni elemento di S' è un divisore di qualche elemento di S allora $A_S = A_{S'}$.

c. Mostrare che se $A_S = A_{S'}$ allora ogni elemento di S' divide qualche elemento di S.

Soluzione.

a. Basta mostrare che

- A_S è un sottogruppo additivo di Q: infatti $0 = \frac{0}{1} \in A_S$. Se $\frac{a}{s} \in A_S$ anche il suo opposto $\frac{-a}{s} \in A_S$ e se $\frac{a}{s}, \frac{a'}{s'} \in A_S$ allora $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'} \in A_S$.
- $1 = \frac{1}{1} \in A_S$ perché $1 \in S$;
- A_S è chiuso rispetto al prodotto: se $\frac{a}{s}, \frac{a'}{s'} \in A_S$ allora $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} \in A_S$.

b. Si ha chiaramente $A_S \subset A_{S'}$ perché $S \subset S'$. Mostriamo l'inclusion opposta e sia quindi $\frac{a}{s'} \in A_{S'}$ per ipotesi sappiamo che esistono $s \in S$ e $b \in A$ tali che $s = bs'$ ma allora
$$\frac{a}{s'} = \frac{ab}{s} \in A_S.$$

c. Sia $s' \in S'$. Per ipotesi abbiamo che $\frac{1}{s'} \in A_S$ per cui esistono $a \in A$ e $s \in S$ tali che $\frac{1}{s'} = \frac{a}{s}$ da cui $s'a = s$ e quindi s' divide s.